REMARKS

The above amendments to the above-captioned application along with the following remarks are being submitted as a full and complete response to the Office Action dated May 21, 2010. In view of the above amendments and the following remarks, the Examiner is respectfully requested to give due reconsideration to this application, to indicate the allowability of the claims, and to pass this case to issue.

Status of the Claims

As outlined above, claims 1-61 stand for consideration in this application, wherein claims 1, 16, 27, 38, 40-42, 46, 55, 57 and 58 are being amended to more particularly point out and distinctly claim the subject invention; and claim 45 is being canceled without prejudice or disclaimer. All amendments to the specification and to the claims are fully supported throughout the disclosure of the invention. Applicants submit that no new matter is being introduced into this application through the submission of this response.

Formality Rejection

Claim 45 is rejected under 35 U.S.C. § 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which Applicants regard as the invention. The Examiner alleges that claim 45 is indefinite regarding the thickness of the RFID reader.

Prior Art Rejections

Claims 1, 5, 11-14, 46, and 56-57 were rejected under 35 U.S.C. §102(e) as being anticipated by Hughes *et al.* (U.S. Patent No. 6,842,106; "Hughes"). Claim 15 was rejected under 35 U.S.C. §103(a) as being unpatentable over Hughes in view of Stewart *et al.* (U.S. Patent No. 6,933,848; "Stewart"). Claim 37 was rejected under 35 U.S.C. §103(a) as being unpatentable over Hughes in view of (U.S. Patent No. 5,850,187; "Carrender") and further in view of Mays *et al.* (U.S. Patent No. 6,838,989; "Mays"). Claims 27-28, 35-36, and 38-44 were rejected under 35 U.S.C. §103(a) as being unpatentable over Hughes in view of Carrender. Claim 61 was rejected under 35 U.S.C. §103(a) as being unpatentable over Hughes in view of

Brown and further in view of Stewart. Applicants have reviewed the above-noted rejections, and hereby respectfully traverse.

The present invention as recited in claim 1 is directed to a contactless communication tag that is attached to a product, the contactless communication tag comprising: a contactless communication unit, which wirelessly exchanges data with a tag reader; a storing unit in which product information and encryption key related information corresponding to the product information are stored; and an encryption unit, which encrypts the product information based on the encryption key related information, wherein the contactless communication unit transmits the encrypted product information and encryption key specifying information to be used in the tag reader to specify the encryption key related information, to the tag reader.

As recited in claim 16, the claimed invention is directed to a contactless communication tag that is attached to a product and provides product information, the contactless communication tag comprising: a contactless communication unit for wirelessly exchanging data with a tag reader; a storing unit for storing product information, encryption key related information, and the number of times the product information is read by the tag reader; an encryption unit for encrypting the product information to be transmitted to the tag reader based on the encryption key related information; and an information providing unit for reading the product information stored in the storing unit in response to a product information request message received from the tag reader, to provide the read product information to the encryption unit, and rejecting provision of the product information to the encryption unit if the number of times the product information is read exceeds a predetermined reference value.

Also, the present invention as recited in claim 27 is directed to a portable tag reader that reads information received from a contactless communication tag, the portable tag reader comprising: a wireless communication unit for wirelessly exchanging data with the contactless communication tag and receiving encrypted product information and encryption key specifying information from the contactless communication tag; a storing unit for storing encryption key related information; a decryption unit for specifying encryption key related information by encryption key specifying information received from the contactless communication tag and decrypting the encrypted product information received from the contactless communication tag based on the specified encryption key related information; and an information reading unit for reading product information decrypted by the decryption unit.

Further, the claimed invention as recited in claim 46 embodies a method of providing product information using a tag reader that communicates with a contactless communication tag, the method comprising: receiving encrypted product information and encryption key specifying information from the contactless communication tag; specifying encryption key related information based on the encryption key specifying information received from the contactless communication tag; decrypting the encrypted product information received from the contactless communication tag based on the specified encryption key related information; and outputting data concerning the decrypted product information.

Even more, the claimed invention as recited in claim 58 embodies a product to which a contactless communication tag is attached, wherein the contactless communication tag comprises: a contactless communication unit, which wirelessly exchanges data with a tag reader; a storing unit in which product information including genuineness information of the product and encryption key related information corresponding to the product information are stored; and an encryption unit, which encrypts the product information based on the encryption key related information, wherein the contactless communication unit transmits the encrypted product information and encryption key specifying information to be used in the tag reader to specify the encryption key related information, to the tag reader, and wherein visible information corresponding to the genuineness information of the product stored in the contactless communication tag is printed on or attached to the product.

In contrast to the present invention, the primary reference of Hughes discloses "a challenged-based tag authentication model" which is a method of securing communications in an RFID system including a reader and an RF tag having a memory configured to store information. The method of Hughes comprises steps of: (a) The reader sends a message to the tag; (b) The tag, in response to the message, generates *a challenge value* and sends the challenge value to the reader; (c) the reader performs a mathematical operation on the challenge value based upon *a key value*, stored in the reader to generate *a challenge reply* and sends the challenge reply to the tag; (d) The tag independently computes *a challenge response* based on an identical key value and mathematical operation stored in the tag, prior to receiving the challenge reply from the reader; (e) The tag compares *the challenge response* computed by the tag with *the challenge reply* sent by the reader; and (f) The tag authenticates the reader if the challenge response matches the challenge reply.

On the other hand, in the present invention, a contactless communication tag stores product information and encryption key related information, encrypts the product information based on the encryption key related information, where the encrypted data is transmitted to a tag reader, which is used *in the tag reader* to confirm whether the product is real or a fake. In particular, a contactless communication tag, such as that recited in independent claims 1 and 58, encrypts product information based on encryption key related information and transmits the encrypted product information and the encryption key specifying information to be used in the tag reader to specify the encryption key related information, to the tag reader. Also, a portable tag reader, such as that recited in independent claims 27 and 46, receives encrypted product information and encryption key specifying information from the tag and decrypts the encrypted product information based on encryption key related information that is specified by the encryption key specifying information received from the tag.

The product information is encrypted by the encryption key related information in the tag. The encryption key specifying information for specifying the encryption key related information are transmitted together with the encrypted product information, from the tag to the tag reader. The tag reader specifies encryption key related information stored therein based on the encryption key specifying information received from the tag, and decrypts the encrypted product information received from the tag based on the specified encryption key related information, thereby confirming whether the product is real or a fake.

Applicants will strongly but respectfully contend that Hughes fails to show or suggest any structure or operation that embodies or incorporates transmitting encryption key specifying information form a tag to a reader and decrypting encrypted product information transmitted from the tag based on encryption key related information specified by the encryption key specifying information transmitted from the tag, thereby authenticating product information of the tag in the reader, as in the claimed invention. Thus, Hughes by itself cannot anticipate or render obvious each and every feature of the claimed invention.

The secondary references of Stewart, Carrender, Mays and Brown were all cited for showing specific features such as those enumerated in the dependent claims. Applicants will contend that none of these references provides any disclosure, teaching or suggestion makes up for the deficiencies in Hughes such that their combination could render all the features of the

claimed invention obvious to those of skill in the art. Rather, even if any or all of the references were combined, Applicant will contend that such a combination would still fall short of showing or suggesting a structure or operation that embodies or incorporates transmitting encryption key specifying information form a tag to a reader and decrypting encrypted product information transmitted from the tag based on encryption key related information specified by the encryption key specifying information transmitted from the tag, thereby authenticating product information of the tag in the reader, as in the claimed invention. The present invention as claimed is distinguishable and thereby allowable over the prior art of record.

Conclusion

In view of all the above, Applicant respectfully submits that certain clear and distinct differences as discussed exist between the present invention as now claimed and the prior art references upon which the rejections in the Office Action rely. These differences are more than sufficient that the present invention as now claimed would not have been anticipated nor rendered obvious given the prior art. Rather, the present invention as a whole is distinguishable, and thereby allowable over the prior art.

Favorable reconsideration of this application as amended is respectfully solicited. Should there be any outstanding issues requiring discussion that would further the prosecution and allowance of the above-captioned application, the Examiner is invited to contact the Applicant's undersigned representative at the address and phone number indicated below.

Respectfully submitted,

Douglas E. Jackson for #28,518

Juan Carlos A. Marquez
Registration Number 34,072

STITES & HARBISON, PLLC
1199 North Fairfax Street
Suite 900
Alexandria, VA 22314-1437
(703) 739-4900 Voice
(703) 739-9577 Fax
Customer No. 38327
August 23, 2010

178969:1:ALEXANDRIA